International Journal of Web Services Research
Volume 20 • Issue 1

Secure Cloud Storage and Retrieval of Personal Health Data From Smart Wearable Devices With Privacy-Preserving Techniques

Zhuolin Mei, Jiujiang University, China
Jing Yu, Jiujiang University, China
Jinzhou Huang, Hubei University of Arts and Science, China*
Bin Wu, Jiujiang University, China
Zhiqiang Zhao, Ningxia Normal University, China
Caicai Zhang, Zhejiang Institute of Mechanical and Electrical Engineering, China
Jiaoli Shi, Jiujiang Key Laboratory of Network and Information Security, China
Xiancheng Wang, Jiujiang University, China
Zongda Wu, Shaoxing University, China

ABSTRACT

With the increasing awareness of personal health, personal health data management has become an important part of people's lives. Smart wearable devices (SWDs) collect people's personal health data, and then store the data on cloud. Authorized entities access the data to provide personalized health services. However, these personal health data contain a large amount of sensitive information, which may pose a significant threat to people's lives and property. To address this, this paper proposes a privacy-preserving solution. SWD data is encrypted, and secure indexes are created using Bloom filter and 0-1 encoding. Encrypted data and indexes are stored in a semi-trusted cloud. Only authorized entities can access the ciphertexts, ensuring secure personalized health management. Extensive experiments validate the scheme's efficiency in index construction, query token generation, and ciphertext search. Security analysis confirms no external entity, including the cloud, gains additional information during retrieval.

KEYWORDS

Cloud Storage, Data Retrieval, Personal Health Data, Privacy Protection, Smart Wearable Device

INTRODUCTION

With the increasing public health awareness, personal health data management is becoming an important component in people's lives (Zeng et al., 2015). Smart wearable devices (SWDs), such as smartwatches, smart bracelets, etc., can collect motion data (such as motion trajectory and status, etc.) and physiological data (such as heart rate and blood pressure, etc.) of the SWD wearer (SWDW)

DOI: 10.4018/IJWSR.331388 *Corresponding Author

anytime and anywhere. In a personal health data management, the data collected by SWDs are typically organized into structured records. For example, data collected by SWDs show that on June 16, 2023, at 8:15 a.m., the SWDW's heart rate was 80 while located at 31°N, 114°E. This information can be represented as a record <2023, 6, 16, 08, 15, 1, 114, 0, 31, 80>, where 1 represents east longitude and 0 represents north latitude. However, due to the small storage space of SWDs and the risk of accidental damage or loss, the collected data are often automatically transmitted to the paired smartphone through a Bluetooth connection and then uploaded to the cloud to obtain unlimited storage space and use the cloud's data backup and disaster recovery mechanisms to ensure that the data are permanently available. In addition, when the data collected by SWDs are uploaded to the cloud as part of electronic health records, medical institutions, insurance companies, or other health management institutions can access and use the data to provide more personalized health management services (Zeng et al., 2018). However, the data collected by SWDs contain sensitive information about the SWDWs. Once this sensitive information is leaked, it may affect personal image, property safety, and even life safety. Therefore, ensuring the security and privacy of sensitive information collected by SWDs and outsourced to the cloud is very important. Encryption is an effective solution to protect the data collected by SWDs. However, traditional encryption methods (e.g., block encryption) cannot support the most common data operations in the cloud, such as ciphertext retrieval (Cui et al., 2023). Although new ciphertext retrieval schemes have been proposed, they have limitations when applied to personal health data management.

The searchable encryption method for numerical data is widely recognized as one of the most effective methods for securely storing and retrieving numerical data (such as time, location, and heart rate collected by SWDs). Efficient searchable encryption methods for numerical data primarily fall into two categories: order-preserving encryption and bucket schemes. Agrawal et al. (2004) propose an order-preserving encryption (OPE) scheme. The main idea of an OPE scheme is to embed order information into the ciphertexts so that the order of the ciphertexts is consistent with that of the plaintexts. Specifically, for any data x>y, it holds Enc(x)>Enc(y), where Enc denotes the encryption algorithm in an OPE scheme. Therefore, an OPE scheme can be used by the cloud to support efficient range queries on ciphertexts. However, most current OPE schemes (Agrawal et al., 2004; Peng et al., 2017; Popa et al., 2011; Quan et al., 2018) only support queries on the ciphertexts of single-dimensional data, and queries on the ciphertexts of personal health data are rarely involved (Zhan et al., 2022). Additionally, since the order information of ciphertexts is revealed in an OPE scheme, attackers can use this information to accurately infer the corresponding plaintexts, leading to potential data security issues (David & Nagaraja, 2004). Another kind of effective method for securely storing and retrieving numerical data is a bucketization scheme (Wang & Ravishankar, 2013; Hore et al., 2004; Hore et al., 2012). In a bucketization scheme, data are divided into multiple buckets, and all data within a bucket are treated as a single unit. A secure encryption scheme is then used to encrypt all the data within each bucket, making the ciphertexts within the same bucket indistinguishable and effectively protecting the order information between them. During ciphertext querying, if the query range intersects with a certain bucket, all the ciphertexts within that bucket are returned as the query result. The number of ciphertexts within each bucket can be adjusted to balance the security of the order information and the accuracy of the query result. To further improve the efficiency of the bucketization scheme, bucketization-based index schemes have been proposed (Wang & Ravishankar, 2013; Mei et al., 2018). However, the scheme in the reference (Wang & Ravishanka, 2013) uses complex matrix calculations, which is not efficient enough. The scheme in the reference (Mei et al., 2018) requires building a tree index (each internal node has n child nodes) over the buckets and works well only for uniformly distributed datasets.

To address the limitations of previous schemes, we propose a Privacy-Preserving Storage and Retrieval Method for Personal Health Data (PPSRMPHD). Our method involves constructing binary trees for the collected data. The security of the binary trees can be ensured by using 0-1 encoding (Gupta & McKeown, 2001) and Bloom filter (Bloom, 1970) techniques. Additionally, SWDs generate